

Copilot in Kirche und Diakonie: Nutzen, Grenzen, Oversharing und die Copilot-Überprüfung vor dem Rollout

Es gibt einen Satz, der in kirchlichen IT-Projekten zuverlässig fällt, meist im vierten Tagesordnungspunkt und immer von jemandem, der gerade einen Vortrag gehört hat: „Können wir das nicht mit Copilot machen?“ Die Antwort lautet überraschend oft: ja. Und sie lautet fast genauso oft: ja, aber nicht in diesem Tenant, nicht mit diesen Berechtigungen und nicht ohne die Mitarbeitervertretung.

Microsoft Copilot – seit dem jüngsten Namenswechsel heißt das frühere Microsoft 365 Copilot schlicht so – ist kein weiterer Chatbot, den man neben Word stellt. Er ist eine Orchestrierungsschicht, die Sprachmodelle mit dem verbindet, was ohnehin schon in Ihrem Tenant liegt: E-Mails, Teams-Chats, SharePoint-Dokumente, Kalender, Besprechungsmitschriften. Genau das macht ihn nützlich. Und genau das macht ihn für kirchliche Träger zu einem Thema, das man nicht nebenbei entscheidet.

Denn kirchliche Träger verarbeiten Daten, die in einem Industriebetrieb schlicht nicht vorkommen. Ein Seelsorgeprotokoll ist keine Projektnotiz. Eine Fallakte aus der Schuldnerberatung ist kein Kundenvorgang. Gemeindegliederdaten aus dem Meldewesen sind kein Adressverteiler. Und die Aufsicht, die im Ernstfall fragt, heißt nicht Landesdatenschutzbeauftragter, sondern Beauftragter für den Datenschutz der EKD oder Diözesandatenschutzbeauftragter.

Dieser Beitrag beschreibt, wo Copilot in Kirche, Diakonie und Caritas tatsächlich Arbeit abnimmt, wo er nichts zu suchen hat, warum das Oversharing-Problem der eigentliche Showstopper ist – und wie eine strukturierte Copilot-Überprüfung vor dem Rollout aussieht. Vorweg die unbequeme Zusammenfassung: Das Copilot-Projekt, das scheitert, scheitert praktisch nie an Copilot. Es scheitert an fünfzehn Jahren SharePoint-Berechtigungen, die nie jemand aufgeräumt hat.

Was Copilot in einem kirchlichen Träger wirklich ist

Der Mechanismus in einem Satz

Copilot beantwortet Fragen, indem er die Anfrage entgegennimmt, im Microsoft Graph nach passendem Material sucht, dieses Material an ein Sprachmodell übergibt und die Antwort mit Quellenangaben zurückliefert. Der entscheidende Schritt ist die Suche, und sie folgt genau einer Regel: Copilot zeigt einer Person ausschließlich Inhalte, für die diese Person mindestens Leseberechtigung hat. Keine Ausnahme, keine Hintertür, kein Sonderindex.

Das klingt beruhigend und ist es auch – solange die Berechtigungen stimmen. Der Satz „Copilot findet nur, was der Nutzer ohnehin sehen darf“ wird gern als Entwarnung vorgetragen. Er ist in Wahrheit eine Diagnose: Copilot macht sichtbar, wie großzügig Ihr Tenant tatsächlich ist. Vorher war zu viel Berechtigung ein theoretisches Problem, weil niemand über 40.000 Dokumente hinweg gesucht hat. Jetzt sucht jemand. Er ist sehr schnell, sehr gründlich und erstaunlich auskunftsfreudig.

Wie Copilot sich in die Gesamtarchitektur eines kirchlichen Tenants einfügt – von der Lizenzierung über die Rechtsgrundlagen bis zur Frage, wer eigentlich Verantwortlicher ist –, ordnet der Überblicksbeitrag [Microsoft 365 in Kirche, Diakonie und Caritas](#) ein. Wer noch grundsätzlicher wissen will, warum ein kirchlicher Tenant anders funktioniert als ein kommunaler, findet die Abgrenzung in [Microsoft 365 in Kirche, Diakonie und Caritas: Was wirklich anders ist als in Kommune und Mittelstand](#). Beides ist hilfreiche Vorlektüre, wenn Copilot gerade auf der Tagesordnung des Leitungsgremiums steht.

Copilot, Copilot Chat und Agenten: drei Dinge, die gern verwechselt werden

In Gesprächen mit Landeskirchenämtern und Generalvikariaten ist die häufigste Verwirrung nicht rechtlicher, sondern begrifflicher Natur. Es gibt nämlich nicht „den Copilot“, sondern mehrere Produkte mit sehr unterschiedlichem Datenzugriff und sehr unterschiedlichen Konsequenzen für Datenschutz und Mitbestimmung.

Variante	Was sie tut	Zugriff auf Tenant-Daten	Was das für Sie heißt
Copilot Chat (im Abonnement enthalten)	Chat mit Sprachmodell, Weboberfläche und Teams-Integration	Grundsätzlich webbasiert; der Zugriff auf Arbeitsinhalte ist der kostenpflichtige Teil	Ist praktisch überall schon da. Braucht eine Regelung, bevor jemand Klientendaten hineinkopiert.
Microsoft Copilot (Lizenz je Person)	Copilot in Word, Excel, Outlook, Teams, PowerPoint, Loop; Besprechungszusammenfassungen	Voller Zugriff auf alles, was die jeweilige Person lesen darf	Das ist die Variante, um die es in diesem Beitrag geht. Hier greift das Oversharing-Thema mit voller Wucht.
Agenten und SharePoint-Agenten	Auf bestimmte Quellen zugeschnittene Assistenten, teils nutzungsbasiert abgerechnet	Auf die konfigurierte Quelle begrenzt, dort aber weiterhin berechtigungsabhängig	Verführerisch einfach zu bauen. Jeder Agent auf einer schlecht berechtigten Site vervielfacht das Problem.
Copilot in Fachanwendungen	KI-Funktionen in KIS, Pflegedokumentation, Fundraising-Software	Kein Microsoft-365-Thema, eigene Vertragslage	Gehört in eine eigene Bewertung. Nicht mit der Microsoft-365-DSFA erschlagen.

Fakten

Was Microsoft für Copilot vertraglich und technisch zusagt – und was davon für kirchliche Träger relevant ist:

- Prompts, Antworten und über Microsoft Graph abgerufene Daten werden nicht zum Training der zugrunde liegenden Sprachmodelle verwendet. Das gilt ausdrücklich auch für die Modelle von Drittanbietern, die als Unterauftragsverarbeiter eingebunden sind.
- Copilot ist für Kunden in der EU ein Dienst innerhalb der EU Data Boundary; EU-Datenverkehr bleibt innerhalb dieser Grenze. Copilot wurde zum 1. März 2024 in die Zusagen zur Datenresidenz

der Produktbestimmungen aufgenommen.

- Ausnahme, die in jede Dokumentation gehört: Modelle, die Anthropic als Unterauftragsverarbeiter bereitstellt, sind derzeit von der EU Data Boundary ausgenommen. Ob diese Modelle genutzt werden, entscheiden Sie als Administrator.
- Copilot zeigt organisationseigene Daten nur Personen, die dafür mindestens Leseberechtigung besitzen. Verschlüsselung durch Purview Information Protection respektiert Copilot ebenfalls: Wer ein Dokument aufgrund eines Labels nicht öffnen darf, bekommt es auch von Copilot nicht.
- Prompts und Antworten werden gespeichert – als Copilot-Aktivitätsverlauf im Tenant, verschlüsselt. Sie sind für Content Search und Purview zugänglich, und Sie können Aufbewahrungsrichtlinien darauf anwenden. Das ist datenschutzrechtlich Segen und Fluch zugleich: nachvollziehbar, aber eben auch vorhanden.
- Die Missbrauchsüberwachung mit menschlicher Sichtung, wie sie in Azure OpenAI grundsätzlich existiert, ist für Copilot-Dienste abgewählt.

Diese Zusagen sind belastbar und sie sind ein guter Ausgangspunkt für das Gespräch mit der Aufsicht. Nur lösen sie das Problem nicht, um das es in kirchlichen Tenants tatsächlich geht. Microsoft sichert zu, die Berechtigungen zu respektieren, die Sie gesetzt haben. Über die Qualität dieser Berechtigungen trifft Microsoft keine Aussage. Das wäre auch vermessen.

Wo Copilot kirchlichen Trägern wirklich hilft

Bevor wir zu den Verboten kommen, der ehrliche Teil: Copilot spart in kirchlichen Verwaltungen real Zeit. Nicht überall, nicht spektakulär, aber an Stellen, an denen seit Jahren Arbeit liegen bleibt, weil niemand Kapazität dafür hat. Kirchliche Verwaltung ist textlastig, formalisiert und wiederholt sich – und genau das ist das Heimspiel eines Sprachmodells.

Protokolle und Gremienarbeit

Presbyterium, Kirchenvorstand, Pfarrgemeinderat, Kreissynode, Verwaltungsrat eines diakonischen Werks, Aufsichtsrat eines Krankenhausverbunds: Kirchliche Träger sind Gremienorganisationen. Wo Gremien tagen, entstehen Protokolle, und Protokolle schreiben ist die undankbarste Aufgabe der Tagesordnung. Copilot kann aus einer Teams-Besprechung eine strukturierte Zusammenfassung mit Beschlüssen und offenen Punkten erzeugen, kann Beschlussvorlagen aus Vorjahresunterlagen fortschreiben und kann prüfen, ob ein Entwurf zur geltenden Ordnung passt.

Zwei Bedingungen, die in der Praxis gern untergehen. Erstens: Die Aufzeichnung oder Transkription einer Gremiensitzung ist eine Verarbeitung personenbezogener Daten und in der Regel mitbestimmungspflichtig, sobald Beschäftigte des Trägers teilnehmen. Zweitens: Nicht jede Gremiensitzung ist protokollfähig. Wenn das Presbyterium über eine Personalangelegenheit oder einen Seelsorgefall spricht, gehört die Transkription abgeschaltet – technisch, nicht durch Appell.

Wie Gremienarbeit in Teams sauber aufgesetzt wird – mit getrennten Bereichen für öffentliche und nichtöffentliche Teile, mit Ehrenamtszugängen und mit einer Ablage, die auch nach der nächsten Wahl noch funktioniert –, ist ein eigenes Thema. Die Tenant-Frage dahinter (eine Struktur für

Gemeinde, Kirchenkreis und Landeskirche oder mehrere) behandelt [Ein Tenant oder viele? Kirchengemeinde, Kirchenkreis, Landeskirche, Bistum und die Frage der Tenant-Architektur](#).

Gemeindebrief, Öffentlichkeitsarbeit und Ehrenamtskommunikation

Der Gemeindebrief ist das dankbarste Copilot-Einsatzfeld überhaupt: Texte ohne besonderen Schutzbedarf, wiederkehrende Formate, chronischer Zeitmangel und häufig ehrenamtliche Redaktion ohne journalistische Ausbildung. Aus einem Veranstaltungshinweis wird ein Ankündigungstext, aus dem Protokoll des Gemeindefests ein Rückblick, aus einem langen Bericht eine Kurzfassung für den Schaukasten. Dasselbe gilt für Pressemitteilungen eines Caritasverbands, für Newsletter eines Bildungswerks und für Anschreiben an Ehrenamtliche.

Die einzige echte Gefahr in diesem Feld ist inhaltlicher Natur: Sprachmodelle formulieren flüssig und faktisch falsch mit derselben Überzeugungskraft. Ein Gemeindebrief mit einem erfundenen Gottesdiensttermin ist kein Datenschutzvorfall, aber ein Vertrauensschaden. Die Regel lautet also: Copilot formuliert, Menschen verantworten. Microsoft formuliert das in der eigenen Dokumentation ungewohnt deutlich – generative Antworten seien nicht garantiert zu hundert Prozent faktentreu.

Anträge an Zuwendungsgeber und Verwendungsnachweise

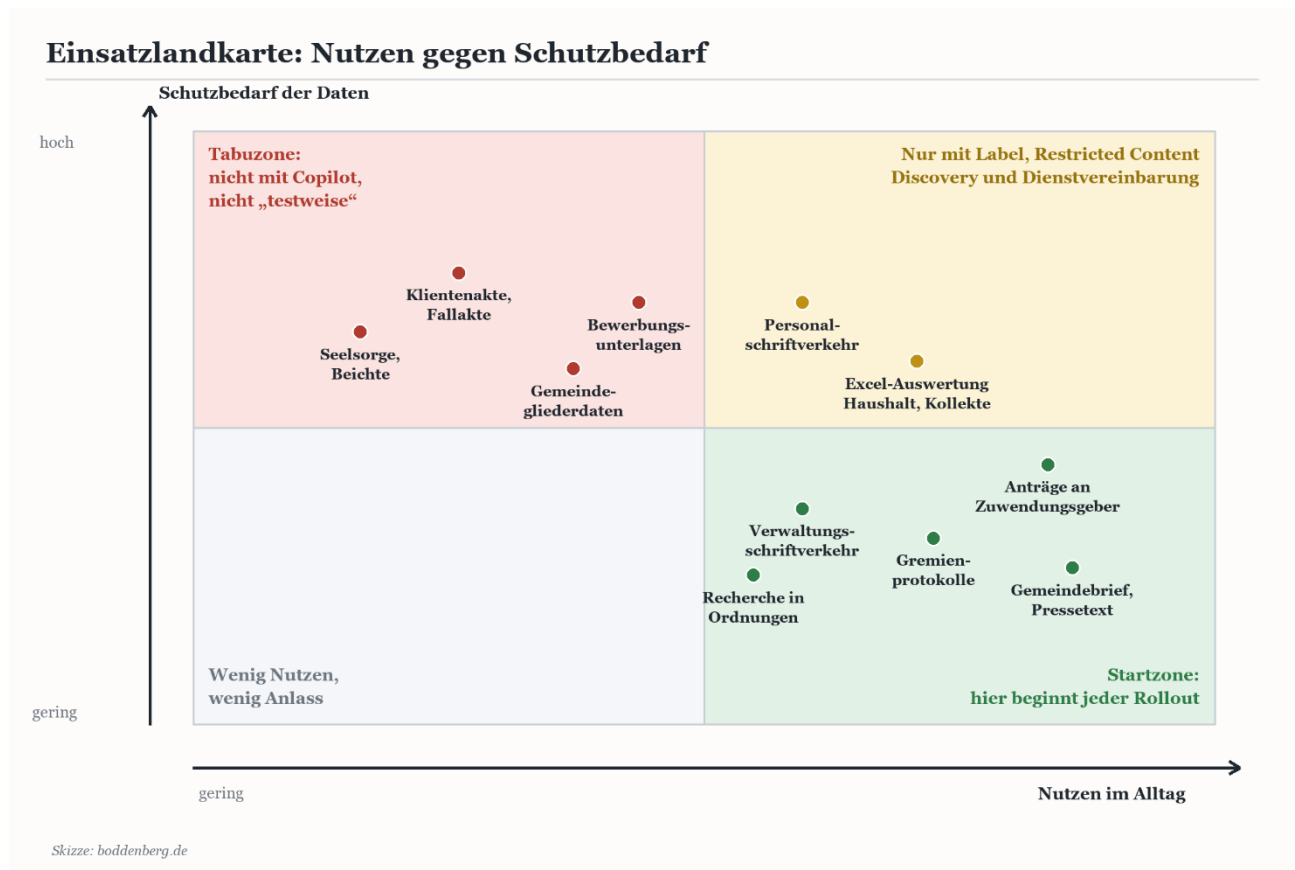
Hier liegt das größte, am seltensten genannte Potenzial. Diakonische Träger und Caritasverbände leben von Anträgen: Landesmittel, Kommunalzuschüsse, Stiftungen, Aktion Mensch, Lotteriemittel, EU-Förderprogramme, Refinanzierung über Leistungsvereinbarungen. Jeder Antrag verlangt dieselben Bausteine in anderer Reihenfolge: Trägerdarstellung, Bedarfsbegründung, Konzeption, Wirkungsziele, Finanzierungsplan, Nachhaltigkeit. Und am Ende steht der Verwendungsnachweis, den niemand freiwillig schreibt.

Ein diakonisches Werk in einer Großstadt hat dafür eine SharePoint-Bibliothek mit rund 200 bewilligten Anträgen aus zwanzig Jahren. Copilot kann dort recherchieren, Formulierungen übernehmen und aus einem Sachbericht die Struktur eines Verwendungsnachweises ableiten. Das ist keine Zukunftsmusik, das ist die Sorte Aufgabe, für die Sprachmodelle gebaut sind. Voraussetzung ist allerdings, dass die Bibliothek keine personenbezogenen Teilnehmerlisten aus den Projekten enthält – und das tut sie fast immer.

Verwaltungsschriftverkehr und Recherche in eigenen Ordnungen

Kirchenkreisverwaltung, Generalvikariat, Landeskirchenamt und Rentamt produzieren Schriftverkehr, der zu neunzig Prozent aus Bausteinen besteht. Bescheide zu Friedhofsgebühren, Anschreiben zur Kirchensteuerverteilung, Stellungnahmen zu Bauanträgen, Auskunft an Kirchengemeinden zu Haushaltsfragen. Copilot in Outlook entwirft, ein Mensch prüft.

Fast noch wertvoller ist die Recherche im eigenen Regelwerk. Kirchliches Recht ist unübersichtlich: Kirchenordnung, Verwaltungsordnung, Haushaltsordnung, Kassationsordnung, Rundschreiben des Landeskirchenamts, Bistumsblatt, dazu AVR und Dienstvereinbarungen. Wer all das in einer gut berechtigten SharePoint-Bibliothek liegen hat, bekommt mit Copilot eine Volltextrecherche mit Quellenangabe, die einem juristischen Referat erstaunlich nahekommt. Mit einer Einschränkung, die man Leitungen vorher sagen sollte: Die Antwort ist ein Rechercheergebnis, keine Rechtsauskunft.



Skizze 1: Einsatzfelder eines kirchlichen Trägers nach Nutzen und Schutzbedarf. Der Rollout beginnt unten rechts – und hört oben links auf.

Einsatzfelder im Überblick

Einsatzfeld	Nutzen	Risiko	Voraussetzung
Gremienprotokolle (Presbyterium, Kirchenvorstand, Pfarrgemeinderat, Kreissynode)	Zusammenfassung, Beschlusslisten, Fortschreibung von Vorlagen; spürbare Entlastung des Ehrenamts	Transkription erfasst auch nichtöffentliche Teile; Personalangelegenheiten landen im Index	Dienstvereinbarung, getrennte Teams für nichtöffentliche Teile, Transkription technisch steuerbar
Gemeindebrief, Pressearbeit, Homepage	Entwürfe, Kürzungen, Zielgruppenvarianten, einfache Sprache	Erfundene Termine und Namen; Bildrechte und Einwilligungen bleiben Menschenaufgabe	Redaktionelle Endabnahme, Schulung der ehrenamtlichen Redaktion
Anträge an Zuwendungsgeber, Verwendungsnachweis e	Wiederverwendung bewilligter Formulierungen, Strukturierung, Fristenübersicht	Alte Antragsordner enthalten Teilnehmerlisten und Fallzahlen	Antragsablage von Projektunterlagen trennen, Bibliothek vorher bereinigen
Verwaltungsschriftverk ehr in Kirchenkreis, Dekanat, Generalvikariat	Entwürfe für Bescheide, Stellungnahmen, Auskunft an Gemeinden	Postfachzugriff macht auch Vertretungsregelungen sichtbar	Postfachberechtigungen prüfen, geteilte Postfächer aufräumen

Recherche in Ordnungen, Satzungen, Rundschreiben	Volltextrecherche mit Quellenangabe über das eigene Regelwerk	Antworten wirken verbindlicher, als sie sind	Regelwerk in eigener, sauber berechtigter Bibliothek; Hinweis auf fehlende Rechtsverbindlichkeit
Auswertungen in Excel (Haushalt, Kollekte, Belegung)	Trends, Vergleiche, Diagramme ohne Formelkenntnis	Zahlen wirken plausibel und sind es nicht immer; Kollektenabrechnung ist prüfungsrelevant	Vier-Augen-Prinzip, keine Weitergabe unbelegter Zahlen an Rechnungsprüfung
Seelsorge und Beichte	Keiner	Bruch des Seelsorgegeheimnisses; strafbewehrt und kirchenrechtlich gravierend	Technische Trennung. Kein Einsatzfeld, unter keiner Bedingung
Klienten- und Fallakten in Beratung, Pflege, Jugendhilfe	Keiner, der das Risiko trägt	Sozialdaten und Schweigepflicht; meldepflichtige Datenpanne bei Fehlkonfiguration	Fachverfahren statt SharePoint; kein Graph-Index auf Fallakten
Personalakten, MAV-Unterlagen	Keiner	MAV-Unterlagen sind dem Dienstgeber entzogen; Personalakten unterliegen eigenen Ordnungen	Eigene Ablage außerhalb des indexierten Bereichs
Meldewesen und Gemeindegliederdaten	Keiner	Kirchenmitgliederdaten sind eigenständig geregelt und gehören nicht in Microsoft 365	Bleiben im Meldewesenverfahren. Punkt

Tipp

Beginnen Sie den Nutznachweis dort, wo die Empfindlichkeit am geringsten und der Frust am größten ist: bei Anträgen und Verwendungsnachweisen. Diese Aufgaben sind textlastig, terminkritisch und werden von Menschen erledigt, die eigentlich für etwas anderes bezahlt werden. Wenn Copilot dort zwei Arbeitstage im Quartal spart, haben Sie eine Zahl, mit der Sie in den Verwaltungsausschuss gehen können – und das ist deutlich überzeugender als eine Produktdemonstration mit generierten Sommerfestplakaten.

Wo Copilot nichts zu suchen hat

Jetzt der Teil, den man in kirchlichen Gremien nicht diplomatisch formulieren sollte, weil Diplomatie hier missverstanden wird. Es gibt Datenbestände in kirchlichen Trägern, bei denen die Frage nach Copilot keine Abwägungsfrage ist. Sie ist eine Frage der Grundausstattung an Verstand.

Drei Datenzonen im kirchlichen Tenant – und was Copilot darin darf



Skizze: boddenberg.de

Skizze 2: Drei Datenzonen im kirchlichen Tenant. Die rote Zone kennt keine Voraussetzungen, unter denen sie grün wird – nur technische Trennung.

Seelsorge und Beichte

Das Seelsorgegeheimnis ist kein gesteigerter Datenschutz. Es ist ein eigenes Rechtsinstitut mit eigener Geschichte und eigener Durchsetzung. Auf evangelischer Seite regelt es das Kirchengesetz zum Schutz des Seelsorgegeheimnisses, das zum 1. Januar 2010 in Kraft getreten ist: Wer sich in einem seelsorglichen Gespräch anvertraut, muss darauf vertrauen können, dass der Inhalt ohne seine Zustimmung nicht an Dritte gelangt; das Beichtgeheimnis ist unverbrüchlich.

Seelsorgerinnen und Seelsorger sind nach diesem Gesetz Geistliche im Sinne der Strafprozessordnung und haben ein Zeugnisverweigerungsrecht. Auf katholischer Seite ist das Beichtiegel im kanonischen Recht absolut geschützt und kennt keine Entbindung, auch nicht durch den Beichtenden selbst.

Übersetzt in Tenant-Sprache: Ein Seelsorgeinhalt, der in OneNote, in einem Teams-Chat oder in einer OneDrive-Datei landet, ist im Microsoft Graph. Er ist damit indexierbar, durchsuchbar, sicherungsfähig, eDiscovery-fähig – und im Zweifel einem Administrator zugänglich. Das steht in direktem Widerspruch zu einem Schutz, der gerade darauf beruht, dass niemand sonst Kenntnis erlangen kann. Die einzige belastbare Antwort ist technische Trennung: Seelsorgedokumentation gehört nicht in den produktiven Microsoft-365-Tenant, und wo sie aus praktischen Gründen doch dort liegt, gehört sie in einen Bereich, der weder indexiert noch von Copilot erreichbar ist.

Klientenakten in Diakonie und Caritas

Schuldnerberatung, Suchtberatung, Schwangerschaftskonfliktberatung, Migrationsdienst, allgemeine Sozialberatung, ambulante Pflege, Eingliederungshilfe, Hilfen zur Erziehung: In diesen Feldern arbeiten kirchliche Träger mit Sozialdaten, mit Gesundheitsdaten und mit Informationen, deren unbefugte Offenbarung für die betroffene Person existenzielle Folgen haben kann. Zusätzlich

gilt für einen Teil der Berufsgruppen eine strafbewehrte Schweigepflicht, die unabhängig vom Datenschutzrecht besteht.

Diese Daten gehören in ein Fachverfahren mit eigenem Rollenkonzept, nicht in eine SharePoint-Bibliothek. Die Praxis sieht leider oft anders aus: Excel-Listen mit Fallnummern, Word-Dokumente mit Gesprächsnotizen, gescannte Bescheide in einem Teams-Kanal, weil das Fachverfahren keine Dokumentenablage hat. Genau diese Schattendokumentation ist es, die Copilot findet.

Personalakten, MAV-Unterlagen und Meldewesen

Personalakten unterliegen in Kirche und Diakonie eigenen Ordnungen und sind in aller Regel einem sehr engen Kreis vorbehalten. Unterlagen der Mitarbeitervertretung sind dem Zugriff des Dienstgebers strukturell entzogen – eine MAV, die ihre Sitzungsprotokolle in einem trägerverwalteten Teams ablegt, hat ein Problem, das mit Copilot nur sichtbar wird. Und Gemeindegliederdaten aus dem kirchlichen Meldewesen folgen einer eigenen Rechtsgrundlage und einer eigenen Verarbeitungslogik; sie sind kein CRM-Datenbestand, den man „mal eben“ für eine Auswertung nach SharePoint exportiert.

Warnung

Ein Copilot-Pilot mit Klientendaten im Testtenant ist kein Pilot. Er ist eine Datenpanne.

Der Satz fällt in Projekten regelmäßig und klingt vernünftig: „Wir spielen einen echten Datenbestand in den Testtenant, sonst sehen wir ja nicht, ob Copilot etwas taugt.“ Rechtlich ist das eine Verarbeitung personenbezogener Daten zu einem neuen Zweck, in einer neuen Umgebung, regelmäßig ohne Rechtsgrundlage, ohne Datenschutz-Folgenabschätzung, ohne Eintrag im Verarbeitungsverzeichnis, häufig ohne Auftragsverarbeitungsvertrag für die Testumgebung und fast immer ohne Beteiligung der Mitarbeitervertretung.

Bei besonders geschützten Daten – Sozialdaten, Gesundheitsdaten, Seelsorgeinhalten – ist der Vorgang damit ein meldepflichtiger Datenschutzverstoß gegenüber dem Beauftragten für den Datenschutz der EKD oder dem zuständigen Diözesandatenschutzbeauftragten. Es gibt dafür keine Testtenant-Ausnahme, keine Pilotprivilegierung und keine „ist ja nur intern“-Klausel.

Der Ausweg ist unspektakulär und funktioniert: synthetische Daten. Erzeugen Sie einen realistischen, aber erfundenen Bestand – fünfzig Anträge, dreihundert Dokumente, ein Dutzend Gremienprotokolle, ein Haushaltsplan, alles frei erfunden. Das kostet zwei Tage und beantwortet dieselben Fragen. Wer behauptet, Copilot lasse sich nur mit Echtdaten bewerten, hat in Wahrheit nur keine Lust auf die zwei Tage.

Das Oversharing-Problem: Copilot findet, was Sie erlaubt haben

Kommen wir zum Kern. Alle bisher genannten Verbote lassen sich durch Disziplin einhalten – solange die Menschen wissen, wo die Grenze verläuft. Oversharing ist heimtückischer, weil niemand etwas falsch macht. Es ist die Summe aus tausend kleinen, jeweils nachvollziehbaren Entscheidungen.

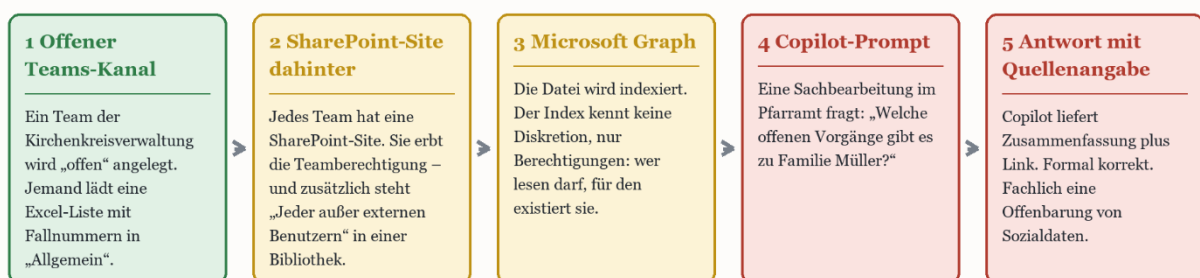
Wie Oversharing in kirchlichen Tenants entsteht

Der typische kirchliche Tenant ist nicht grün auf der Wiese entstanden. Er ist aus einer Dateiserver-Migration hervorgegangen, meist unter Zeitdruck, oft während der Pandemie, gelegentlich von einem Systemhaus, das „erst mal alles hochziehen“ als Migrationsstrategie verstanden hat. Die typischen Muster:

- Die Freigabe „Jeder außer externen Benutzern“ wurde gesetzt, damit „die Kollegen dran kommen“. Sie steht heute auf Bibliotheken, deren Inhalt sich in fünf Jahren vollständig geändert hat.
- Teams wurden „öffentlich“ angelegt, weil das die Standardeinstellung war und „privat“ nach Geheimniskrämerei klang. Jedes Team bringt eine SharePoint-Site mit.
- Die Dateiserver-Struktur wurde eins zu eins übernommen, inklusive der Ordner „Alt“, „Alt_2“ und „Sicherheit Frau K.“, in denen Personalvorgänge und Beratungsnotizen friedlich nebeneinanderliegen.
- Freigabelinks vom Typ „Personen in der Organisation“ wurden verschickt, weil das Anlegen einer Berechtigungsgruppe drei Klicks mehr gekostet hätte.
- Sites haben keinen Eigentümer mehr, weil die Person, die sie angelegt hat, längst in einer anderen Einrichtung arbeitet oder im Ruhestand ist.
- Kirchenkreis und Kirchengemeinden teilen sich einen Tenant, und die Trennung zwischen Trägerebenen wurde nie sauber modelliert.

Jeder einzelne Punkt ist harmlos, solange Suche bedeutet, dass jemand den richtigen Dateinamen kennen muss. Copilot ändert diese Voraussetzung vollständig. Er sucht semantisch, über alle Quellen hinweg, ohne dass die fragende Person auch nur ahnen muss, dass es diese Ablage gibt.

Der Oversharing-Pfad: vom offenen Teams-Kanal zur Copilot-Antwort



Der Punkt, an dem die meisten Projekte stolpern

Copilot hat nichts geknackt. Kein Angriff, keine Lücke, kein Schaden am Tenant. Copilot hat nur getan, was das Berechtigungsmodell erlaubt – und in gewachsenen SharePoint-Landschaften erlaubt es regelmäßig deutlich mehr, als irgendjemand je entschieden hat. Oversharing ist kein Copilot-Problem. Copilot ist nur der erste Nutzer, der es bemerkt.

Skizze: boddenberg.de

Skizze 3: Der Oversharing-Pfad. Fünf unauffällige Schritte, an deren Ende eine Sozialdatenoffenbarung steht – ohne dass irgendetwas kaputt war.

Ein katholischer Krankenhausverbund mit mehreren Standorten hat genau diesen Weg durchlaufen, allerdings mit gutem Ausgang: Die Auffälligkeit wurde in der Pilotgruppe entdeckt, nicht im Regelbetrieb. Eine Qualitätssicherung hatte in einem Teams-Kanal eine Auswertung mit Fallnummern abgelegt. Copilot zitierte sie korrekt, vollständig und mit Link. Der Pilot wurde

gestoppt, die Berechtigungen wurden aufgeräumt, der Rollout kam ein halbes Jahr später. Genau so soll ein Pilot funktionieren – und genau deshalb gehören keine Echtdata mit Personenbezug hinein, wenn man das Risiko nicht tragen will.

Die Werkzeuge, die Microsoft dafür mitliefert

Die gute Nachricht: Microsoft hat das Problem verstanden und liefert ein ordentliches Instrumentarium. Die weniger gute: Es ist über SharePoint Advanced Management, Purview und die Tenant-Einstellungen verteilt, und die wirkungsvollsten Werkzeuge setzen eine Copilot-Lizenz voraus – Sie brauchen also die Lizenz, bevor Sie feststellen können, ob Sie bereit für die Lizenz sind. Ein bemerkenswertes Geschäftsmodell.

Werkzeug	Was es tut	Wofür es in kirchlichen Trägern taugt	Haken
Content Management Assessment	Geführte Bewertung des Tenants mit Befunden zu überbreiten Freigaben, inaktiven und eigentümerlosen Sites	Der beste Einstieg. Liefert eine Befundliste, mit der man in die Leitungsrunde gehen kann	Teil von SharePoint Advanced Management; sinnvoll alle 30 Tage wiederholen
Berichte zur Datenzugriffsverwaltung	Momentaufnahmen zu Site-Berechtigungen, Bericht zu „Jeder außer externen Benutzern“, Auswertung erzeugter Freigabelinks	Findet genau die Muster, die in migrierten Tenants entstehen	Die Aktivitätsberichte betrachten die letzten 28 Tage und die Top-Sites – kein vollständiges Inventar
Bericht „Site-Berechtigungen für Benutzer“	Listet alle Sites auf, die eine bestimmte Person erreichen kann	Unschlagbar für die Frage der MAV: „Was sieht diese eine Person eigentlich?“	Erzeugt Diskussionen, die man aushalten muss
Restricted Access Control	Begrenzt den Zugriff auf eine Site auf eine Sicherheitsgruppe – wer nicht darin ist, kommt nicht hinein, auch nicht über alte Links	Beratungsstellen, Personalbereich, Gremien mit nichtöffentlichen Teilen	Greift hart. Vorher prüfen, wer legitim Zugriff braucht
Restricted Content Discovery	Nimmt Inhalte einer Site aus Copilot und aus der organisationsweiten Suche heraus, ohne die Berechtigungen zu ändern	Das Mittel der Wahl für die gelbe Zone: zugänglich, aber nicht auffindbar	Seit 2026 auch auf Site-Ebene delegierbar und um zuletzt verwendete Dateien erweitert
Restricted SharePoint Search	Erlaubnisliste mit maximal 100 Sites; nur diese sind für Copilot und die Tenant-Suche breit erreichbar	Notbremse für den Start, wenn die Aufräumarbeit noch läuft	Von Microsoft ausdrücklich als kurzfristige Lösung bezeichnet, nicht als Dauerzustand
Purview Sensitivity Labels	Klassifizierung und Verschlüsselung; Copilot respektiert die Nutzungsrechte aus dem Label	Das eigentliche Rückgrat eines kirchlichen Schutzkonzepts	Braucht ein durchdachtes Label-Konzept, sonst labelt jeder alles „vertraulich“

Purview DSPM for AI	Zeigt, welche KI-Anwendungen genutzt werden und welche sensiblen Inhalte in Prompts auftauchen; Risikobewertungen zum Oversharing	Die laufende Überwachung nach dem Rollout – und ein gutes Argument gegenüber der Aufsicht	Auswertung von Nutzung ist mitbestimmungsrelevant. Vorher mit der MAV klären
Microsoft 365 Archive und Lebenszyklusrichtlinien	Inaktive und eigentümerlose Sites erkennen, archivieren, Eigentümer bestätigen lassen	Räumt die Altlasten der Dateiserver-Migration ab	Archivierte Inhalte sind für Nutzer nicht mehr erreichbar – Kassationsordnung beachten

Tipp

Die wirksamste Maßnahme steht in keiner Produktbeschreibung: Benennen Sie für jede SharePoint-Site und jedes Team eine verantwortliche Person mit Namen, und lassen Sie diese Person jährlich schriftlich bestätigen, wer Zugriff hat und warum. Die Attestierungsrichtlinien in SharePoint machen daraus einen automatisierten Vorgang. In einer Organisation, die Visitation, Rechnungsprüfung und Jahresbericht ohnehin kennt, ist das kulturell anschlussfähig – anders als in vielen Unternehmen, wo genau diese Frage als Misstrauen gelesen wird.

Recht, Mitbestimmung und der Weg zum Rollout

DSG-EKD und KDG: die Folgenabschätzung ist keine Kür

Kirchliche Träger unterliegen nicht der Datenschutz-Grundverordnung in ihrer staatlichen Anwendung, sondern eigenem Recht: auf evangelischer Seite dem Kirchengesetz über den Datenschutz der EKD, auf katholischer Seite dem Gesetz über den Kirchlichen Datenschutz. Beide sind der Grundverordnung nachgebildet, aber eben nicht identisch – und vor allem haben sie eine eigene Aufsicht.

Für Copilot zentral ist die Datenschutz-Folgenabschätzung. Sowohl das DSG-EKD in § 34 als auch das KDG in § 35 verlangen sie, wenn eine Verarbeitungsform – ausdrücklich einschließlich des Einsatzes neuer Technologien – aufgrund von Art, Umfang, Umständen und Zwecken voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Beide Vorschriften verlangen dieselben vier Bestandteile: systematische Beschreibung der Verarbeitung und ihrer Zwecke, Bewertung von Notwendigkeit und Verhältnismäßigkeit, Bewertung der Risiken für die betroffenen Personen und die geplanten Abhilfemaßnahmen samt Garantien und Sicherheitsvorkehrungen.

Ein KI-System, das quer über alle Dokumente, E-Mails und Chats eines diakonischen Trägers greift, erfüllt dieses Kriterium zuverlässig. Die Diskussion „brauchen wir dafür wirklich eine Folgenabschätzung?“ können Sie sich sparen. Der Beauftragte für den Datenschutz der EKD hat übrigens die Orientierungshilfe der staatlichen Datenschutzkonferenz zu Künstlicher Intelligenz vom Mai 2024 aufgegriffen und ausdrücklich als Leitfaden auch für Kirche und Diakonie

empfohlen – ein nützlicher Hinweis, weil er zeigt, dass die kirchliche Aufsicht hier nicht auf einer Sonderdogmatik besteht.

Was DSGVO-EKD und KDG jeweils konkret für einen Microsoft-365-Tenant bedeuten, ist in zwei eigenen Beiträgen ausgeführt: [DSGVO-EKD verständlich: Was das evangelische Datenschutzgesetz für Microsoft 365 konkret bedeutet](#) und [KDG verständlich: Microsoft 365 unter dem Kirchlichen Datenschutzgesetz der katholischen Kirche](#). Was BfD EKD, Diözesandatenschutzbeauftragte und das Katholische Datenschutzzentrum in der Prüfpraxis tatsächlich sehen wollen, beschreibt [Kirchliche Datenschutzaufsicht in der Praxis: Was BfD EKD und Diözesandatenschutzbeauftragte von einem Microsoft-365-Tenant erwarten](#).

MVG-EKD und MAVO: ohne MAV kein Copilot

Der Dritte Weg bedeutet nicht weniger Mitbestimmung, sondern andere. Wo im Betrieb der Betriebsrat und in der Kommune der Personalrat sitzt, sitzt beim kirchlichen Träger die Mitarbeitervertretung – auf evangelischer Seite nach dem Mitarbeitervertretungsgesetz der EKD, auf katholischer Seite nach der Mitarbeitervertretungsordnung des jeweiligen Bistums.

In beiden Ordnungen ist die Einführung und Anwendung technischer Einrichtungen, die geeignet sind, das Verhalten oder die Leistung der Mitarbeiterinnen und Mitarbeiter zu überwachen, mitbestimmungspflichtig: im MVG-EKD in § 40 als Mitbestimmung in organisatorischen und sozialen Angelegenheiten, in der MAVO in § 36 als Zustimmungserfordernis. Entscheidend ist dabei ein Punkt, den Dienstgeber gern übersehen: Es kommt nicht darauf an, ob Sie überwachen wollen. Die kirchliche Rechtsprechung legt den Tatbestand so aus, dass die objektive Eignung zur Überwachung genügt.

Copilot ist objektiv geeignet. Die Nutzungsdaten laufen im Audit-Log auf, Purview DSPM for AI wertet Prompts aus, und die Copilot-Nutzungsberichte im Admin Center zeigen personenbezogen, wer wie häufig welche Funktion verwendet. Damit ist die Mitbestimmung eröffnet, unabhängig von Ihren Absichten. Die Frage ist also nicht ob, sondern wann Sie die MAV einbinden – und die Antwort lautet: bevor die Lizenzen bestellt sind, nicht danach.

Eine Dienstvereinbarung zu Copilot regelt in der Praxis mindestens: zulässige und unzulässige Einsatzfelder, ein ausdrückliches Verbot der Leistungs- und Verhaltenskontrolle, den Umgang mit Besprechungstranskripten, die Aufbewahrungsdauer des Copilot-Aktivitätsverlaufs, die Freiwilligkeit der Nutzung, Schulung als Voraussetzung für die Lizenzzuweisung und ein Verfahren zur Überprüfung nach sechs oder zwölf Monaten. Erfreulicherweise ist der Gestaltungsspielraum groß – und eine MAV, die man früh beteiligt, ist in kirchlichen Trägern erfahrungsgemäß eher Verbündeter als Gegner.

Wie Sie MVG-EKD und MAVO im Microsoft-365-Kontext praktisch handhaben, wo Beteiligungsrechte genau ansetzen und wie eine tragfähige Dienstvereinbarung zu Teams, Copilot und Protokollierung aufgebaut ist, behandelt [Mitarbeitervertretung und Microsoft 365: MVG-EKD, MAVO, Dienstvereinbarung und Mitbestimmung bei Teams, Copilot und Protokollierung](#) ausführlich.

Wichtig

Die drei Formalien, die im Copilot-Projekt am häufigsten vergessen werden – und die in jeder

aufsichtlichen Prüfung als Erstes abgefragt werden:

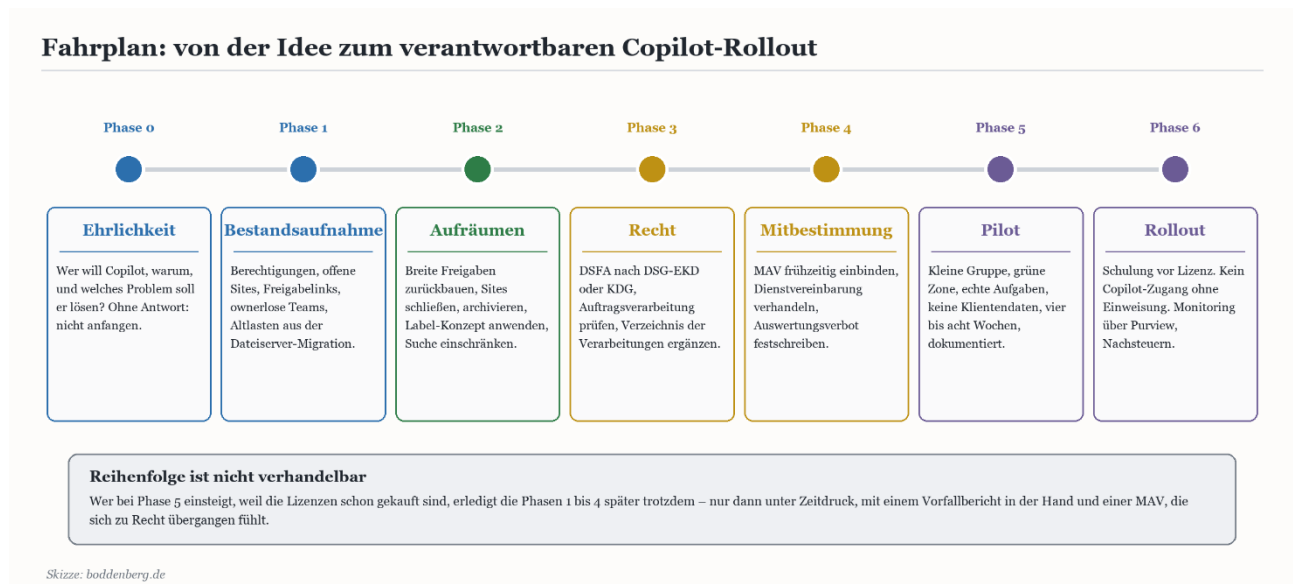
1. Das Verarbeitungsverzeichnis. Copilot ist keine Variante einer bestehenden Verarbeitung, sondern eine eigene. Er gehört als eigener Eintrag hinein, mit Zweck, Kategorien betroffener Personen, Empfängern und Löschfristen für den Aktivitätsverlauf.
2. Die Auftragsverarbeitung. Der bestehende Vertrag mit Microsoft deckt Copilot als Bestandteil der Online-Dienste ab; das entbindet nicht davon, die Unterauftragsverarbeiter zu prüfen – insbesondere die Frage, welche Modelle Sie zulassen und welche davon außerhalb der EU Data Boundary arbeiten. Diese Entscheidung treffen Sie als Administrator, also ist sie auch Ihre Entscheidung.
3. Die Information der Belegschaft. Dass Prompts und Antworten gespeichert werden und über Purview zugänglich sind, ist kein Detail für die IT. Es gehört in die Datenschutzinformation für die Beschäftigten – und es beruhigt spürbar, wenn man gleich dazusagt, dass jede Person ihren eigenen Aktivitätsverlauf selbst löschen kann.

Die Copilot- und Oversharing-Überprüfung vor dem Rollout

Alles bisher Gesagte läuft auf eine einzige Frage hinaus, die vor der Lizenzentscheidung beantwortet gehört: Was würde Copilot in diesem Tenant morgen früh finden, wenn ihn jemand danach fragte? Diese Frage lässt sich nicht schätzen und nicht aus dem Bauch beantworten. Sie lässt sich messen.

Eine strukturierte Copilot- und Oversharing-Überprüfung nimmt sich den Tenant in seiner tatsächlichen Verfassung vor: Berechtigungsstruktur über alle Sites, Bestand an breiten Freigaben und Freigabelinks, eigentümerlose und inaktive Sites, Gastzugänge, Postfachberechtigungen und Vertretungsregelungen, vorhandene oder fehlende Klassifizierung, Zustand der Teams-Landschaft, Auffindbarkeit von Inhalten mit besonderem Schutzbedarf, Zustand von Audit und Aufbewahrung. Am Ende steht kein Werkzeugbericht, sondern eine priorisierte Befundliste mit Maßnahmen, Aufwandschätzung und einer belastbaren Aussage zur Frage, ob und unter welchen Bedingungen ein Rollout verantwortbar ist – in einer Form, die Sie dem Leitungsgremium, der MAV und der Aufsicht vorlegen können.

Diese Überprüfung ist Teil des Angebots für kirchliche Träger: [Microsoft-365-Beratung für kirchliche Träger](#). Dort finden Sie den Umfang, den Ablauf und die Festpreiskonditionen der Copilot- und Oversharing-Überprüfung sowie der übrigen Bausteine – von der Datenschutz-Folgenabschätzung bis zur Begleitung der Dienstvereinbarung. Der Aufwand liegt je nach Größe des Tenants typischerweise im Bereich weniger Tage, und er liegt in jedem Fall deutlich unter dem Aufwand einer Meldung an die kirchliche Aufsicht.



Skizze 4: Der Fahrplan vom Copilot-Wunsch zum verantwortbaren Rollout. Sieben Phasen, von denen die ersten fünf regelmäßig übersprungen werden sollen.

Was ein Pilot leisten muss – und was nicht

Ein Copilot-Pilot in einem kirchlichen Träger hat drei Aufgaben, und keine davon lautet „beweisen, dass die Technik funktioniert“. Die Technik funktioniert. Die Fragen sind andere: Erstens, ob die Zeitersparnis in konkreten kirchlichen Arbeitsabläufen groß genug ist, um die Lizenzkosten gegenüber dem Verwaltungsausschuss zu rechtfertigen. Zweitens, ob das Schutzkonzept aus Labels, Zugriffsbeschränkungen und Suchbegrenzung im Alltag trägt oder ob es umgangen wird. Drittens, welcher Schulungsbedarf tatsächlich besteht – und der ist in Pfarrämtern, Kitas und Pflegediensten regelmäßig höher, als IT-Leitungen vermuten.

Ein brauchbarer Pilot umfasst zehn bis fünfundzwanzig Personen aus unterschiedlichen Bereichen, läuft vier bis acht Wochen, arbeitet ausschließlich in der grünen Zone und dokumentiert Ergebnisse in einer Form, die später in die Folgenabschätzung und in die Dienstvereinbarung einfließen kann. Wer zusätzlich eine Kontrollgruppe ohne Lizenz mitlaufen lässt, hat am Ende sogar Zahlen statt Eindrücke.

Häufige Fragen

Ist Copilot nach DSGVO-EKD und KDG überhaupt zulässig?

Ja, grundsätzlich. Weder das DSGVO-EKD noch das KDG verbieten den Einsatz von KI-Systemen. Beide verlangen Rechtsgrundlage, Zweckbindung, Datenminimierung, technische und organisatorische Maßnahmen und – bei voraussichtlich hohem Risiko – eine Datenschutz-Folgenabschätzung. Der Einsatz ist damit an Bedingungen geknüpft, nicht ausgeschlossen. Unzulässig wird er dort, wo er auf Datenbestände trifft, die eigenen Schutzregimen unterliegen – Seelsorgegeheimnis, Schweigepflicht, Meldewesen.

Verlassen unsere Daten die EU?

Für Kunden in der EU ist Copilot ein Dienst innerhalb der EU Data Boundary; EU-Datenverkehr bleibt innerhalb dieser Grenze, und Copilot ist seit dem 1. März 2024 in die Datenresidenzzusagen der Produktbestimmungen einbezogen. Eine Ausnahme müssen Sie kennen und dokumentieren: Modelle, die Anthropic als Unterauftragsverarbeiter bereitstellt, sind derzeit von der EU Data Boundary ausgenommen. Ob diese Modelle in Ihrem Tenant genutzt werden, ist eine administrative Entscheidung – und in einem kirchlichen Träger eine, die dokumentiert und mit der örtlich Beauftragten oder dem örtlich Beauftragten für den Datenschutz abgestimmt gehört.

Werden unsere Dokumente zum Training verwendet?

Nein. Microsoft sagt zu, dass Prompts, Antworten und die über Microsoft Graph abgerufenen Daten nicht zum Training der zugrunde liegenden Sprachmodelle verwendet werden; das gilt ausdrücklich auch für die Modelle der eingebundenen Drittanbieter. Die optionale Feedbackfunktion ist davon zu unterscheiden – sie lässt sich über Administratoreinstellungen steuern, und in einem kirchlichen Tenant spricht einiges dafür, sie abzuschalten.

Wir haben Copilot Chat doch sowieso schon. Reicht das nicht?

Copilot Chat ist in den gängigen Microsoft-365-Abonnements enthalten und damit in praktisch jedem kirchlichen Tenant bereits vorhanden. Genau das ist der Punkt, den viele Träger übersehen: Sie haben bereits eine KI-Anwendung im Haus, ob Sie darüber entschieden haben oder nicht. Was Copilot Chat in der enthaltenen Form nicht leistet, ist die Verknüpfung mit Ihren Arbeitsinhalten – das ist der lizenzpflichtige Teil. Handlungsbedarf besteht trotzdem sofort: Eine Regelung, was Beschäftigte in einen Chat kopieren dürfen, brauchen Sie heute, nicht erst mit der ersten Lizenz.

Was ist mit Ehrenamtlichen?

Ehrenamtliche sind der wunde Punkt jeder kirchlichen Berechtigungsdiskussion. Sie arbeiten in Gremien mit, oft über Gastzugänge oder geteilte Postfächer, und sie sind arbeitsrechtlich nicht eingebunden. Wenn ein Gastzugang Zugriff auf eine Site hat, sieht die Person diese Inhalte – und wenn sie eine Copilot-Lizenz hätte, fände Copilot sie auch. Die Regel ist einfach: Ehrenamtliche bekommen keine Copilot-Lizenz, und ihre Zugänge gehören in die Überprüfung mit derselben Gründlichkeit wie Beschäftigtenkonten. Der häufigste Befund ist übrigens nicht ein zu weit reichender Gastzugang, sondern ein Gastzugang, der seit drei Jahren hätte gelöscht werden müssen.

Muss die MAV zustimmen oder nur informiert werden?

Es geht um Mitbestimmung, nicht um Information. Sowohl das MVG-EKD in § 40 als auch die MAVO in § 36 erfassen die Einführung und Anwendung technischer Einrichtungen, die zur Überwachung von Verhalten oder Leistung geeignet sind; nach kirchlicher Rechtsprechung genügt die objektive Eignung, eine Überwachungsabsicht ist nicht erforderlich. Copilot erfüllt das über Nutzungsberichte, Audit-Log und Prompt-Auswertung. Praktisch heißt das: ohne Dienstvereinbarung kein Rollout. Und ohne frühe Beteiligung dauert die Dienstvereinbarung länger als der technische Teil des Projekts.

Wie viel Aufräumarbeit steht uns bevor?

Das hängt an der Entstehungsgeschichte des Tenants, nicht an seiner Größe. Ein 2023 sauber aufgebauter Tenant einer Landeskirche kann in wenigen Wochen bereit sein. Ein aus einer Dateiserver-Migration hervorgegangener Tenant eines Caritasverbands auf Kreisebene mit gewachsener Ordnerstruktur braucht mehrere Monate, und die Arbeit ist nicht delegierbar: Ob eine Bibliothek noch gebraucht wird, weiß nur der Fachbereich. Die Erlaubnisliste der eingeschränkten SharePoint-Suche mit maximal hundert Sites ist die Brücke für diese Zeit – von Microsoft ausdrücklich als kurzfristige Lösung gedacht, nicht als Dauerzustand.

Lohnt sich Copilot bei kirchlichen Nonprofit-Konditionen überhaupt?

Die Lizenzfrage ist eine eigene Rechnung, und sie fällt selten eindeutig aus. Wichtig ist die Reihenfolge: Erst klären, welche Personengruppen überhaupt in Frage kommen – Verwaltung und Leitung ja, Frontline-Arbeitsplätze in Pflege und Kita in aller Regel nicht –, dann den Nutzen für genau diese Gruppen bewerten, dann lizenzieren. Ein Rollout „für alle“ ist in kirchlichen Trägern praktisch nie wirtschaftlich, und er ist auch nicht nötig: Der Nutzen konzentriert sich stark auf textlastige Verwaltungsrollen.

Was, wenn Copilot etwas findet, das er nicht finden sollte?

Dann haben Sie zwei Vorgänge, die Sie auseinanderhalten müssen. Der erste ist technisch: Zugriff beschränken, Restricted Content Discovery setzen, Berechtigungen bereinigen, dokumentieren. Der zweite ist rechtlich: Prüfen, ob eine meldepflichtige Verletzung des Schutzes personenbezogener Daten vorliegt. Bei Sozialdaten, Gesundheitsdaten oder Seelsorgeinhalten lautet die Antwort in aller Regel ja, und dann läuft eine kurze Frist gegenüber dem Beauftragten für den Datenschutz der EKD beziehungsweise dem zuständigen Diözesandatenschutzbeauftragten. Dass Copilot den Fund gemacht hat und nicht ein Angreifer, ändert an der Meldepflicht nichts – wohl aber an der Bewertung, denn ein selbst entdeckter und sauber dokumentierter Befund wird von jeder Aufsicht anders gelesen als ein Hinweis von außen.

Fazit

Copilot ist für kirchliche Träger weder Heilsversprechen noch Teufelszeug. Er ist ein nützliches Werkzeug für eine klar umrissene Menge von Aufgaben – Protokolle, Gemeindebrief, Anträge an Zuwendungsgeber, Verwaltungsschriftverkehr, Recherche im eigenen Regelwerk – und ein erhebliches Risiko für eine ebenso klar umrissene Menge von Datenbeständen, bei denen die Antwort schlicht Nein lautet.

Dazwischen liegt das eigentliche Projekt, und es hat mit Künstlicher Intelligenz wenig zu tun. Es besteht darin, die Berechtigungen im eigenen Tenant so in Ordnung zu bringen, wie sie immer hätten sein sollen. Copilot stellt diese Aufgabe nur unangenehm scharf: Er beantwortet Fragen auf der Grundlage dessen, was Sie erlaubt haben – und das erste Mal, dass jemand systematisch prüft, was das eigentlich ist, sollte nicht der Regelbetrieb sein.

Die Reihenfolge ist deshalb nicht verhandelbar: erst messen, dann aufräumen, dann die Folgenabschätzung, dann die MAV, dann der Pilot ohne Echtdaten, dann die Lizenzen. Wer diese Reihenfolge umdreht, erledigt dieselben Schritte trotzdem – nur unter Zeitdruck, mit einem

Vorfallbericht in der Hand und vor einer Aufsicht, die zu Recht fragt, warum das nicht vorher passiert ist. Und die Dienstgemeinschaft, auf die sich kirchliche Träger gern berufen, besteht nicht zuletzt darin, dass die Menschen, deren Daten hier verarbeitet werden, sich darauf verlassen können, dass jemand vorher nachgesehen hat.

Weiter

- › [Microsoft 365 in Kirche, Diakonie und Caritas – der Überblick zur gesamten Serie](#)
- › [Mitarbeitervertretung und Microsoft 365: MVG-EKD, MAVO, Dienstvereinbarung und Mitbestimmung bei Teams, Copilot und Protokollierung – Mitbestimmung, Beteiligungsrechte und Dienstvereinbarung im Detail](#)
- › [DSG-EKD verständlich: Was das evangelische Datenschutzgesetz für Microsoft 365 konkret bedeutet](#)
- › [KDG verständlich: Microsoft 365 unter dem Kirchlichen Datenschutzgesetz der katholischen Kirche](#)
- › [Kirchliche Datenschutzaufsicht in der Praxis: Was BfD EKD und Diözesandatenschutzbeauftragte von einem Microsoft-365-Tenant erwarten](#)
- › [Ein Tenant oder viele? Kirchengemeinde, Kirchenkreis, Landeskirche, Bistum und die Frage der Tenant-Architektur](#)
- › [Die Cloud-Frage in der Kirche: Kirchliche Rechenzentren, Microsoft 365 und die Ehrlichkeit über Datenstandorte](#)
- › [Microsoft-365-Lizenzierung für kirchliche Träger: Nonprofit-Angebote, Frontline-Pläne und die Frage, wer überhaupt berechtigt ist](#)
- › [Microsoft 365 Einführungskonzept für kirchliche Träger: Die Kirchenedition zum Festpreis](#)
- › [Kirche, Diakonie, Caritas: DSG-EKD, KDG und MAV in Microsoft 365](#)
- › [Microsoft-365-Schulung für kirchliche Träger – weil Schulung vor Lizenz kommt, nicht danach](#)